Cryptojacking - Cryptomining in the browser

Published
November 10, 2017

Introduction

Cryptomining (http://chimera.labs.oreilly.com/books/1234000001802/ch02.html#_mining_transactions_in_blocks) is the process by which cryptocurrency transactions are verified and added to a public ledger, known as the blockchain (https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchain). At the same time cryptomining is also the mean by which new cryptocurrency coins are released. Cryptomining is profitable for its operator. One of the latest trends in this area is Coinhive, a legitimate piece of code that performs cryptomining in browsers. Coinhive is used by website owners as an alternative source of income in addition to other sources, e.g. advertisement, pay-per-click, etc.

Although web site owners should obtain the consent of end-users before deploying Coinhive, it often runs without user consent and without the option to opt-out, hence maliciously exploiting the computing resources of end-users. In the meantime, malicious agents have been misusing Coinhive by injecting the code in compromised web sites, browser extensions, and mobile applications. Consequently, they abuse users' computing power to perform cryptomining on their behalf. From the end-user point of view it makes not much difference whether Coinhive is abused by cyber criminals or by website owners deploying it without their consent.

What is cryptomining?

Cryptocurrencies are underpinned by a technology named blockchain (https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchain). Blockchain is a public ledger shared amongst a network of computers and consists of all transactions that have taken place using a certain cryptocurrency. Transactions are validated and stored in the blockchain through a process called mining (cryptomining). Mining is done by certain peers of the cryptocurrency network who compete (individually or in groups) in solving a difficult mathematical problem, called *proof-of-work*. This problem requires significant computational power to be solved. The node or group of nodes solving the problem first gets to add the latest batch of completed transactions in the blockchain and receives a reward for the performed computation (in cryptocurrency coins). Mining requires the use of special software for solving the mathematical problem.

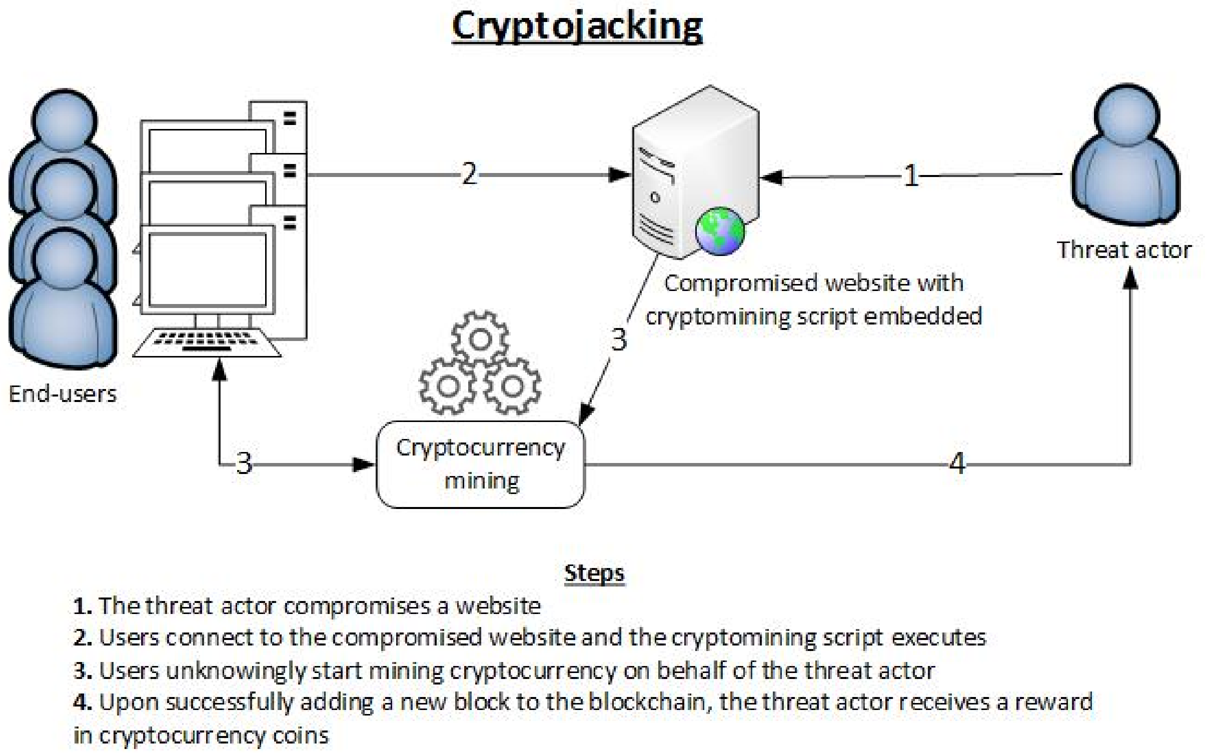
Coinhive: Cryptomining in the browser

In September 2017, a company introduced Coinhive (https://coinhive.com/), which mines the cryptocurrency Monero (XMR). Coinhive, is a piece of code written in JavaScript; website owners can simply embed it in their website. Coinhive introduced a new business model for websites. It claims that website owners can remove ads from their websites, load Coinhive instead, and while users are simply browsing the website, mine for Monero. In that way, website owners can supposedly still make profit and support their businesses, without bothering their visitors with advertisements.

When users access a website with Coinhive embedded, Coinhive initiates the process of cryptomining on behalf of the website owner by using user system resources. The visitors of a website represent the group of nodes doing the intensive computational work to solve the mathematical problem. But, instead of them receiving the reward when solving the challenge, the website owner receives it. Moreover, in cases of abuse, i.e. when cyber criminals inject the cryptomining script in compromised websites, cyber criminals receive the reward. Due to Coinhive's resonance (resulting from both legitimate and illegal use cases) more software similar to Coinhive emerged (https://twitter.com/bad_packets/status/918713647894953984).

Cryptomining abuse

The technique of hijacking browsers for mining cryptocurrency (without user consent) is called "cryptojacking (https://go.malwarebytes.com/rs/805-USG-300/images/Drive-by_Mining_FINAL.pdf)". Delivering cryptocurrency miners through malware is nothing new. Yet, mining cryptocurrency when accessing a webpage is new and it has already been abused and rapidly spread. The figure below illustrates how cyber criminals abuse cryptomining scripts through cryptojacking. Cryptojacking also refers to legitimate websites that do not explicitly ask visitors' consent prior to executing cryptomining scripts in their browsers, nor do they provide them the option to opt-out.



Steps

1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Several cases of cryptomining abuse have been spotted:

- **Coinhive injected into websites.** Pirate Bay, a notorious piracy website is one of the first websites spotted (https://www.bleepingcomputer.com/news/security/psa-the-pirate-bay-is-running-an-in-browser-cryptocurrency-miner-with-no-opt-out/) of deliberately using Coinhive. The issue was that it was done transparently, without the visitors' consent. Once the cryptomining script was discovered, Pirate Bay issued a statement mentioning that it was testing this solution as an alternative revenue source. Following the Pirate Bay news, two "Showtime" domains were spotted (https://www.bleepingcomputer.com/news/security/showtime-websites-used-to-mine-monero-unclear-if-hack-or-an-experiment/) loading and running Coinhive. It is unclear whether this was deliberate, or the website was compromised. Politifact was another case (https://techcrunch.com/2017/10/13/surreptitious-cryptocurrency-miners-hide-on-politifact-and-hundreds-of-other-sites/?ncid=rss) of a website serving Coinhive to its visitors, while also unknown whether it was done deliberately or not. According to a recent study (https://blog.adguard.com/en/crypto-mining-fever/) these websites are not the only ones; a big number of websites seem to have been running Coinhive (https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores/) or a similar JavaScript-based cryptomining software without user consent.

- **Coinhive injected into compromised websites.** Researchers identified (https://blog.sucuri.net/2017/09/hacked-websites-mine-crypocurrencies.html) compromised (https://www.linkedin.com/pulse/so-how-many-hacked-websites-already-using-coinhive-alexandros) Wordpress and Magento websites that had Coinhive or a similar JavaScript-based miner injected into them.
- **Coinhive injected into browser extensions.** Besides websites, there were (https://www.bleepingcomputer.com/news/security/chrome-extension-embeds-in-browser-monero-miner-that-drains-your-cpu/) cases (https://medium.com/@ale_polidori/with-this-article-i-would-like-to-share-a-real-experience-of-discovering-a-malware-that-mines-36e26c8dfe1e) of web browser extensions embedding Coinhive. In such cases the cryptomining software run in the background and mined "Monero" while the browser was running -and not only when visiting a specific website. This is a more persistent way of cryptojacking.
- **Coinhive deployed with malware.** Another case of Coinhive abuse is that of Coinhive being deployed alongside malware. A researcher found (https://twitter.com/malwrhunterteam/status/911644745608433664?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwww.bleepingcomputer.com%2Fnews%2Fsecurity%2Fcoinhive-is-rapidly-becoming-a-favorite-tool-among-malware-devs%2F) a site serving a fake Java update. The site was also mining for Monero using Coinhive.
- **Android Coinhive cryptomining malware.** A security researcher spotted (https://twitter.com/virqdroid/status/925336630948454400) an Android variant of Coinhive targeting Russian users. Additional (http://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/?utm_source=hs_email&utm_medium=email&utm_content=58156607&_hsenc=p2ANqtz-_kvkM1CjJCGX7DgRlzJh9lv2v26MoBiadQLriwC-ZI5biD2l_Q75BpGNvoWX6Vd-KT-fUprTumIFEjyQlGebdw8WrjVg&_hsmi=58156607) Android applications using a cryptomining scripts were recently identified (https://www.ixiacom.com/company/blog/everythings-better-blockchain) suggesting that this trend is currently expanding to mobile applications as well.
- **Typosquatted domains embedding Coinhive.** Someone registered (https://www.bleepingcomputer.com/news/security/coinhive-is-rapidly-becoming-a-favorite-tool-among-malware-devs/) the "twitter.com.com" domain and loaded Coinhive to it. Essentially, users who mistyped Twitter's URL and landed on that webpage would mine Monero for the domain owner for as long as they remained at the webpage.
- **Malvertising campaigns and Coinhive.** Security experts found (http://blog.trendmicro.com/trendlabs-security-intelligence/eitest-campaign-uses-tech-support-scams-deliver-coinhives-monero-miner/) that one of the biggest malvertising groups was also deploying Coinhive through malicious advertisments. Malicious advertisements redirected users to tech support scams, while Coinhive was loaded in the browser and mined for Monero at the same time.
- **Coinhive deployed through hijacked cloud services.** Security researchers reported that developers and organizations are not properly securing their cloud services, e.g. AWS, Azure and Google Cloud Platform systems, thus allowing cyber criminals to hijack (https://www.theregister.co.uk/2017/10/17/cryptocoin_miners_turning_up_on_unprotected_cloud_instances/) them and use them to mine cryptocurrency. It's most probable that threat actors got access to these systems by using default credentials.
- **Coinhive variations.** Microsoft notified (https://twitter.com/msftmmpc/status/924921349755342848) of variations (https://twitter.com/msftmmpc/status/922728149015826432) of Coinhive being spotted (https://twitter.com/msftmmpc/status/919831580184645632) in the wild. Such a development indicates that Coinhive's success has motivated the emergence of similar software by other parties that want to join this market.

What can be done about it?

- **User consent and opt-out option.** After the extensive abuse of Coinhive, the company behind it, released a new version called “Authedmine”, which explicitly requires user consent before initiating cryptomining. Legitimate businesses that choose solutions similar to Coinhive should request user consent before running any cryptomining code in their browsers, while offering them the option to opt-out too.
- **Consider using an ad-blocker.** Well known ad-blockers quickly added support for blocking Coinhive. Hence users that make use of ad-blockers should not worry about cryptomining JavaScript running in the background. Having said that, while ad-blockers can be beneficial against unwanted and often malicious advertisements and scripts, they can also be damaging for legitimate companies whose revenue relies on advertisements. Therefore, users may still use an ad-blocker but whitelist websites accordingly.
- **Consider using a browser extension for blocking cryptomining scripts.** Developers have also created browser extensions that block Coinhive and other similar cryptomining scripts. Users can search for these extensions in their browsers’ market place.
- **Update your antivirus/anti-malware software.** Antivirus and anti-malware solutions already block cryptomining software, hence users are advised to keep them updated at all times.
- **Disable unnecessary browser extensions.** Users are advised to disable/remove browser extensions they no longer use as it is often the case that a legitimate extension becomes malicious after an update (https://www.enisa.europa.eu/publications/info-notes/malware-in-browser-extensions). Hence, it is recommended to reduce the attack surface whenever possible by keeping installed extensions to a minimum.
- **Consult ENISA’s Threat Landscape report.** More recommendations against malware can be found in ENISA’s Threat Landscape (https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016).

Closing Remarks

Cryptojacking quickly became a new tool in the hands of cyber criminals, which shows once more that cyber criminals are ready to find novel ways and grasp new opportunities to make profit in very short time. First (https://torrentfreak.com/how-much-money-can-pirate-bay-make-from-a-cryptocoin-miner-170924/) indications (https://blog.adguard.com/en/crypto-mining-fever/) suggest that cyber criminals have already made profit out of this scheme with almost zero cost. This, implies that they will keep abusing this method as long as it remains profitable. As past cases have shown, it would be no surprise to witness the combination of such a scheme with different types of cyber threats, e.g. phishing, ransomware etc. hence vigilance is advised.

References

- Mining transactions in blocks (http://chimera.labs.oreilly.com/books/1234000001802/ch02.html#_mining_transactions_in_blocks)
- Blockchain (resolveuid/b886cdb9c3134b81b68f07d2dd80e187)
- Coinhive (https://coinhive.com/)
- Coinhive alternatives (https://twitter.com/bad_packets/status/918713647894953984)
- Drive-by-mining (https://go.malwarebytes.com/rs/805-USG-300/images/Drive-by_Mining_FINAL.pdf)
- The Pirate bay is running an in-browser cryptocurrency miner with no opt-out (https://www.bleepingcomputer.com/news/security/psa-the-pirate-bay-is-running-an-in-browser-cryptocurrency-miner-with-no-opt-out/)
- Showtime websites used to mine Monero (https://www.bleepingcomputer.com/news/security/showtime-websites-used-to-mine-monero-

unclear-if-hack-or-an-experiment/)

- Surreptitious cryptocurrency miners hide on Politifact (https://techcrunch.com/2017/10/13/surreptitious-cryptocurrency-miners-hide-on-politifact-and-hundreds-of-other-sites/?ncid=rss)
- Cryptocurrency mining affects over 500 million people (https://blog.adguard.com/en/crypto-mining-fever/)
- Cryptojacking found on 2496 online stores (https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores/)

Show 17 more